

## CLAIMS

1. A method for classifying a message, comprising:  
extracting a plurality of reference points;  
classifying the plurality of reference points; and  
5 detecting that the message is a phish message based on the classified  
reference points.
2. A method for classifying a message as recited in Claim 1, wherein classifying the  
plurality of reference points including looking up the plurality of reference points in a  
database.
- 10 3. A method for classifying a message as recited in Claim 1, wherein detecting that  
the message is a phish message includes determining that the message includes divergent  
reference points.
4. A method for classifying a message as recited in Claim 1, wherein detecting that  
the message is a phish message includes determining that the plurality of reference points  
15 includes a first reference point to a first source and a second reference point to a second  
source.
5. A method for classifying a message as recited in Claim 1, wherein detecting that  
the message is a phish message includes determining that the plurality of reference points  
includes a first reference point to a legitimate source and a second reference point to a  
20 questionable source.
6. A method for classifying a message as recited in Claim 1, wherein detecting that  
the message is a phish message includes determining that the plurality of reference points

includes a first reference point to a first source and a second reference point to a second source, and the second reference point is intended to appear as a reference to the first source.

7. A method for classifying a message as recited in Claim 1, further comprising  
5 computing a thumbprint of the message and storing the thumbprint to a database.

8. A method for classifying a message as recited in Claim 1, further comprising  
computing a thumbprint of the message and storing the thumbprint to a database; wherein  
the database is shared.

9. A method for classifying a message as recited in Claim 1, further comprising  
10 identifying a plurality of fraud indicators and applying a statistical analysis on the  
plurality of fraud indicators.

10. A method for classifying a message as recited in Claim 1, further comprising  
quarantining the message.

11. A method for classifying a message as recited in Claim 1, further comprising  
15 deleting the message.

12. A method for classifying a message as recited in Claim 1, further comprising  
providing an alert to a recipient of the message.

13. A method for classifying a message as recited in Claim 1, further comprising  
providing an alert to a recipient indicating that the message is a phish message.

20 14. A method for classifying a message as recited in Claim 1, further comprising  
providing an explanation of the phish message to a recipient.

15. A method for classifying a message, comprising:  
identifying a plurality of fraud indicators in the message;

applying a statistical analysis on the plurality of fraud indicators; and  
determining whether the message is a fraudulent message based on the  
analysis.

16. A method for classifying a message as recited in Claim 15, wherein identifying  
5 the plurality of fraud indicators includes identifying a raw Internet protocol (IP) address.

17. A method for classifying a message as recited in Claim 15, wherein identifying  
the plurality of fraud indicators includes identifying non-standard encoding in the  
message.

18. A method for classifying a message as recited in Claim 15, wherein identifying  
10 the plurality of fraud indicators includes identifying a link with an embedded user name.

19. A method for classifying a message as recited in Claim 15, wherein identifying  
the plurality of fraud indicators includes identifying a misleading link.

20. A method for classifying a message as recited in Claim 15, wherein identifying  
the plurality of fraud indicators includes identifying a mismatched link name.

15 21. A method for classifying a message as recited in Claim 15, wherein identifying  
the plurality of fraud indicators includes identifying a form in the message.

22. A method for classifying a message as recited in Claim 15, wherein identifying  
the plurality of fraud indicators includes identifying a form in the message that requests  
special information.

20 23. A method for classifying a message as recited in Claim 15, wherein identifying  
the plurality of fraud indicators includes identifying suspect content in the message.

24. A method for classifying a message as recited in Claim 15, wherein applying a statistical analysis on the plurality of fraud indicators includes obtaining a score based on the fraud indicators.

25. A system for classifying a message, comprising:

5                   a processor configured to extract a plurality of reference points, classify the plurality of reference points, and detect that the message is a phish message based on the classified reference points; and

                  a memory coupled with the processor, wherein the memory is configured to provide the processor with instructions.

10 26. A computer program product for classifying a message, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

                  extracting a plurality of reference points;

                  classifying the plurality of reference points; and

15                   detecting that the message is a phish message based on the classified reference points.

27. A system for classifying a message, comprising:

                  a processor configured to identify a plurality of fraud indicators in the message, apply a statistical analysis on the plurality of fraud indicators and

20                   determine whether the message is a fraudulent message based on the analysis; and

                  a memory coupled with the processor, wherein the memory is configured to provide the processor with instructions.

28. A computer program product for classifying a message, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

- identifying a plurality of fraud indicators in the message;
- 5 applying a statistical analysis on the plurality of fraud indicators; and
- determining whether the message is a fraudulent message based on the analysis.